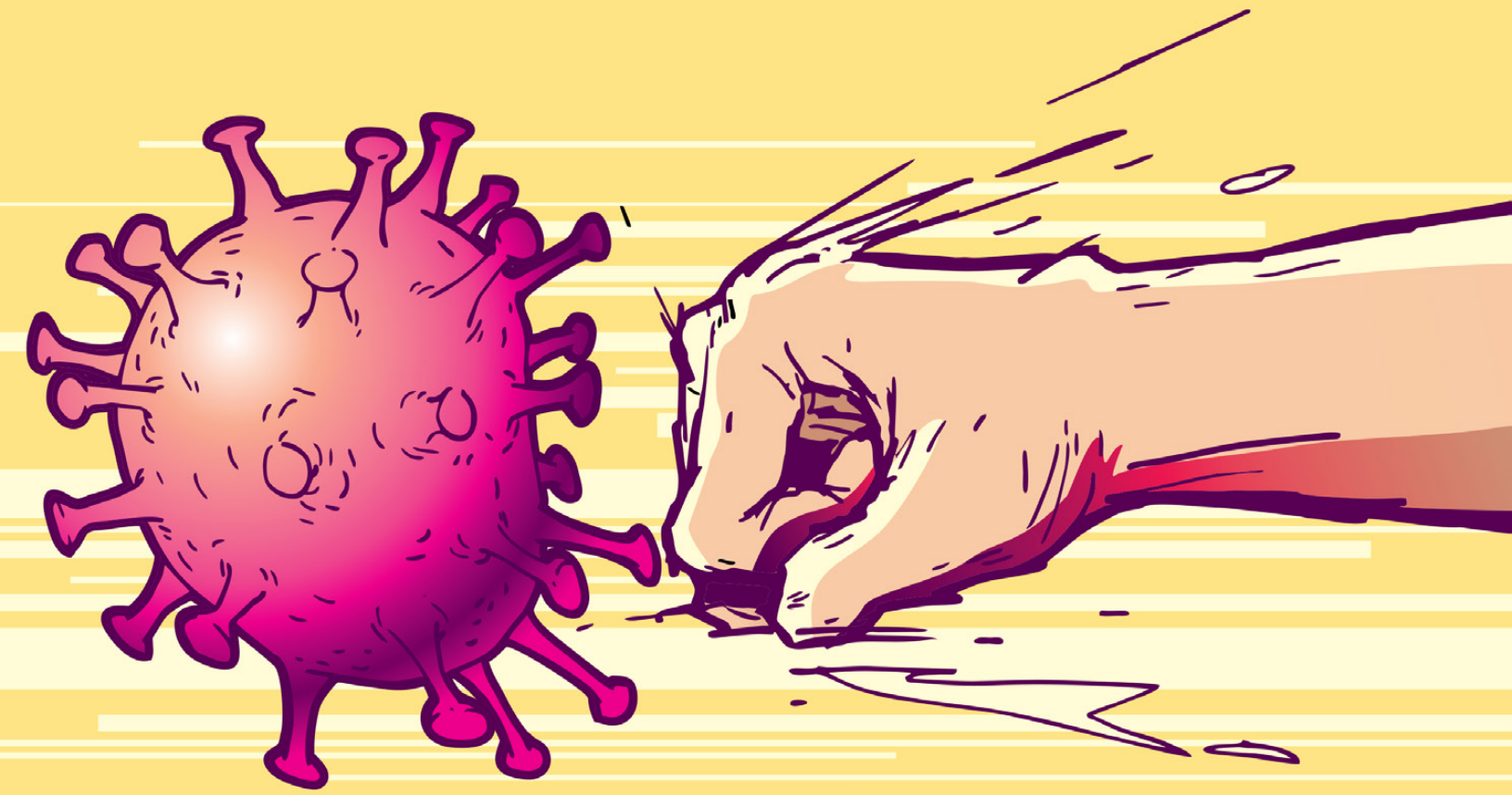
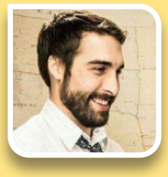
THE PANDEMIC, EDTECH, AND THE TRICKY SUBJECT OF SERVICE PROVIDERS AND PROCESSORS



BY CODY VENZKE[1]



1 Cody J. Venzke is a Policy Counsel at the Center for Democracy & Technology and focuses on privacy, technology, and data in education. The views expressed in this article are exclusively those of the author and do not necessarily reflect those of the Center for Democracy & Technology. This article has been prepared for informational purposes only and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers.

CPI ANTITRUST CHRONICLE
JANUARY 2021

I. INTRODUCTION

With the onset of the global coronavirus pandemic, the use of technology in education has seen a rapid transformation. Schools implemented remote learning in response to the pandemic and, instead of learning in classrooms, children began learning online, a trend that has extended well into the new school year. With the movement of children's learning and data online, privacy concerns began to multiply. Advocates called attention to data use and security vulnerabilities in education technology ("edtech") platforms. That concern was shared by the California Attorney General's Office, which was responsible for the newly enforceable California Consumer Privacy Act ("CCPA").[2] Early in the pandemic, the Attorney General stated, "Whether it's our children's schooling, socializing with family and friends, or working remotely – we are turning to mobile phones and computers as a lifeline. With such a dependency on online connectivity, it is more important than ever for Californians to know their privacy rights."[3]

The CCPA shares a number of similarities[4] with the European Union's General Data Protection Regulation ("GDPR").[5] Both regulations, for example, enable individuals to be notified about companies' data collection and data use practices, to review the data collected, and to seek its correction or deletion.[6] Nonetheless, the two laws are not identical, and untangling their application to schools and edtech vendors can be complicated. As described below, that applicability depends not only on the data these entities collect, but about whom they collect it, where they do business, and their roles as principals or agents in the data processing lifecycle.

This paper examines the landscape of edtech in the pandemic, the geographic and substantive applicability of the CCPA and the GDPR, both laws' tangled provisions governing principals and agents in the data lifecycle, and the significance of those provisions for the exercise of individuals' data rights.

2 Cal. Civil Code. §§ 1798.100-.199.

3 Attorney General Press Office, *Attorney General Becerra Reminds Consumers of their Data Privacy Rights During the COVID-19 Public Health Emergency*, State of California Department of Justice (Apr. 10, 2020), https://oag.ca.gov/news/press-releases/attorney-general-becerra-reminds-consumers-their-data-privacy-rights-during.

4 See DataGuidance & Future of Privacy Forum, *Comparing Privacy Laws: GDPR vs. CCPA* (Dec. 18, 2019), available at https://fpf.org/2019/12/18/comparing-privacy-laws-gdpr-v-ccpa/.

5 Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, General Data Protection Regulation, 2016 OJ (L 119) 1 [hereinafter GDPR].

6 See DataGuidance & Future of Privacy Forum, *supra* note 4.

II. LANDSCAPE OF EDTECH BEFORE, DURING, AND AFTER THE PANDEMIC

Edtech vendors provide technology products for schools, families, and parents to help support learning in and outside of the classroom. With the onset of the pandemic, edtech became synonymous with the videoconferencing platforms of Zoom Video Communications, Inc., and other companies as students and teachers increasingly relied on them to connect.[7] Videoconferencing, however, represents only one sliver of the broader edtech market, with products available to aid students' writing, to provide modules for teaching and assessing, to maintain student records and credentials, and to recruit employees and postsecondary students.[8]

The edtech market drives both investment and data collection. In 2018, new U.S. investments in edtech platforms exceeded $1 billion, with $333 million invested in edtech for K-12 institutions, $463 million in edtech for postsecondary institutions, and $437 in informal learning.[9] Within K-12 investment in 2018, $148 million was invested in technology supporting school operations, $95 million in supporting teacher needs, and $90 million in providing curriculum,[10] with the majority of the investment in curriculum-related technology flowing to language arts and language learning.[11] Investment is expected to increase, especially in adult education and outside of the United States as part of the continued growth of the education sector in general and the continued effects of the pandemic specifically.[12] The pandemic in particular has driven a spike in edtech adoption, with the number of different edtech tools in use jumping from 703 per month to 1,327 — a ninety percent increase.[13]

The increased investment in and adoption of edtech has driven data collection and usage by schools and vendors — and with it, privacy concerns.[14] Educational institutions have long collected student data to assess and monitor student achievement, but technology has made it possible to collect and connect new dimensions of data. For example, the California Cradle-to-Career Data System will combine data from K-12 schools, colleges and universities, employers, and social services to track the effectiveness of education programs in helping students secure places in the workforce.[15] Data and the edtech that facilitates its collection and sharing may also help schools assess gaps in equity, access to technology, and educational opportunity.[16]

However, privacy concerns have accompanied that data collection and sharing and have prompted calls for policy reforms to address the new challenges of emerging education technology.[17] The primary U.S. federal student privacy law, the Family Educational Rights and Privacy Act (FERPA),[18] was passed in 1974, long before the rise of edtech and big data and in many ways did not anticipate the prominent role of tech-

7 Patrick Wall, *With Cell Phones and Laptops, Newark Teachers Stay Connected with Students During School Shutdown*, Chalkbeat (Mar. 19, 2020), https://newark.chalkbeat.org/2020/3/19/21196078/with-cell-phones-and-laptops-newark-teachers-stay-connected-with-students-during-school-shutdown.

8 See Simran Mahanty, *Top 25 SaaS EdTech Companies in 2020*, SmartKarrot (Sept. 18, 2020), https://www.smartkarrot.com/resources/blog/top-edtech-companies-startups/.

9 EdSurge, *Preparing for Impact: What's Changing in Edtech Investment*, State of Edtech 2019, https://www.stateofedtech2019.com/ (last visited Nov. 30, 2020).

10 *Id.*

11 EdSurge, *K-12 Curriculum*, State of Edtech 2019, https://www.stateofedtech2019.com/curriculum (last visited Nov. 30, 2020).

12 Mike Dolan, *Big Funds Circle EdTech as Post-Pandemic Mega-Trend* (Sept. 25, 2020), https://www.nasdaq.com/articles/column-big-funds-circle-edtech-as-post-pandemic-mega-trend-%3Amike-dolan-2020-09-25.

13 Michele Molnar, *Number of Ed-Tech Tools in Use Has Jumped 90 Percent Since School Closures*, EdWeek Market Brief (July 8, 2020), https://marketbrief.edweek.org/marketplace-k-12/access-ed-tech-tools-jumped-90-percent-since-school-closures.

14 Alyson Klein, *Here's How Districts Should Handle Privacy Considerations in the COVID Era*, EdWeek (Oct. 27, 2020), http://blogs.edweek.org/edweek/DigitalEducation/2020/10/covid-privacy-districts-technology.html; Dominic Dhil Panakal, *School Stakeholders Navigating Student Privacy*, National Law Review (Oct. 29, 2020), https://www.natlawreview.com/article/school-stakeholders-navigating-student-privacy.

15 WestEd, *California Cradle-to-Career Data System*, California Data System, https://cadatasystem.wested.org/ (last visited Nov. 30, 2020).

16 Sam Peterson, *Why Teachers Need Interoperability—Whether They Know It or Not*, EdSurge (Oct. 27, 2020), https://www.edsurge.com/news/2020-10-27-why-teachers-need-interoperability-whether-they-know-it-or-not.

17 See Cheri Kiesecker, *A Privacy Blueprint for Biden*, Parent Coalition for Student Privacy (Nov. 11, 2020), https://www.studentprivacymatters.org/a-privacy-blueprint-for-biden; Faith Boninger et al, *Asleep at the Switch: Schoolhouse Commercialism, Student Privacy, and the Failure of Policymaking*, National Education Policy Center (Aug. 15, 2017), https://nepc.colorado.edu/publication/schoolhouse-commercialism-2017.

18 20 U.S.C. § 1232g.

nology and data in education.[19] Consequently, the CCPA and the GDPR, tailored for data collection and sharing by "advanced technologies" and "sophisticated algorithms,"[20] may seem like strong candidates to address the privacy concerns raised by edtech and data collection in schools.

Those laws, however, have specific and sometimes idiosyncratic provisions governing their applicability based on geography, substance, and edtech vendors' relationships to the schools they serve. Schools and vendors should be especially cognizant of the laws' differing applications to principals and agents in the data lifecycle and for- and non-profit entities.

III. GEOGRAPHIC AND SUBSTANTIVE SCOPE

The GDPR and the CCPA both contain provisions governing their geographic reach and substantive scope — that is, the type of entities they apply to and the information and individuals they protect. Those provisions depend not only where individuals subject to data collection are located, but where edtech vendors conduct their business, and on the type of data they are collecting.

A. Geographic & Substantive Scope of the GDPR

The GDPR applies to two sets of entities with ties to the European Union. First, it applies to entities in the European Union that process personal data, regardless of where the processing takes place.[21] That scope includes both entities and their agents — labeled data "controllers" or "processors" — with "an establishment" in the Union.[22] Second, the GDPR applies to controllers and processors outside the Union if they process the data of "data subjects" or natural persons within the Union, so long as that processing is related to either offering goods or services to or monitoring the behavior of data subjects in the Union.[23]

The focus of those protections is "personal data." Under the GDPR, "personal data" is any information "relating" to a data subject; a "data subject" is any "identified or identifiable natural person."[24] That definition does not contain a citizenship requirement and consequently, the scope of the GDPR's protections is not limited to residents or citizens of the Union, but any natural person physically in the Union.[25] "Processing" means any "operation" on personal data such as collecting, using, disclosing, or deleting data — roughly analogous to each stage in various formulations of the data lifecycle.[26]

The GDPR's substantive scope encompasses education data. Both schools and edtech vendors will hold personal data that relates to identifiable natural persons such as transcripts, performance metrics, demographic information, applications for admission, employee personnel files, and medical records. Critically, the GDPR applies to more than schools physically *in* the Union but also to schools that collect personal data *from* persons in the Union. That scope might include North American universities that collect applications from prospective students in the Union, maintain files on employees there, or send students to study abroad in the Union.[27] Edtech vendors, however, do not necessarily collect personal data on their own initiative, but do so on behalf of schools. Consequently, their obligations under the GDPR depend on the GDPR's two-tiered distinction between principals and agents in the data lifecycle, or "controllers" and "processors," discussed in detail below.

19 Owasso Independent School Dist. No. I-011 v. Falvo, 534 U.S. 426. 434-35 (2002) ("Congress contemplated that education records would be kept in one place with a single record of access. . . . FERPA implies that education records are institutional records kept by a single central custodian, such as a registrar . . . .").

20 AB 375 Senate Floor Analysis, S. 2017-2018 at 6 (June 28, 2018), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375#.

21 GDPR art. 3(1).

22 GDPR art. 3(1).

23 GDPR art. 3(2).

24 GDPR art. 4(1); see Laura Jehl & Alan Friel, *CCPA and GDPR Comparison Chart*, BakerHostetler LLP (2018), https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf.

25 GDPR rec. 14 ("The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data.").

26 E.g., UNICEF & Gov Lab, Responsible Data for Children: Synthesis Report at 7 (2019), available at https://rd4c.org/files/rd4c-report-final.pdf (listing planning, colleting, storing and preparing, sharing, analyzing, and using); *Data Lifecycle*, U.S. Geological Survey, https://www.usgs.gov/products/data-and-tools/data-management/data-lifecycle (last visited Nov. 26, 2020) (planning, acquiring, processing, analyzing, preserving, and sharing).

27 See *General Data Protection Regulation (GDPR)*, New York University, https://www.nyu.edu/life/information-technology/it-security-and-policies/general-data-protection-regulation.html (last visited Dec. 1, 2020).

B. Geographic & Substantive Scope of the CCPA

The CCPA has a similar broad reach beyond the borders of its enacting jurisdiction. The CCPA applies to any "business" that is organized for profit, does business in California, "collects consumers' personal information or on the behalf of which that information is collected," and "determines the purposes and means of the processing of consumers' personal information."[28] Under the CCPA, a "consumer" is any "natural person who is a California resident."[29] Thus, like the GDPR, the CCPA is applicable even to businesses not physically in the state so long as it does business there. Unlike the GDPR, however, the CCPA protects only permanent residents, including when they are temporarily outside the state[30]; its protections do not extend to all natural persons "in" the jurisdiction, such as temporary residents and visitors.[31]

Like the GDPR's "personal data," the CCPA defines "personal information" broadly. Its definition includes information that "could reasonably be linked, directly or indirectly, with a particular consumer," paralleling the standard definition of personal information as information that is "linkable" to a particular person.[32] The CCPA, however, expands this definition, including "information that identifies, relates to, describes, is reasonably capable of being associated with" a household or consumer. Although that definition extends beyond mere identification or linkability,[33] neither the California Attorney General nor the courts have clarified its boundaries. The CCPA's definition of "personal information" includes a non-exhaustive list of examples, including "[e]ducation information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act."[34]

Despite its explicit application to education information, the CCPA does not necessarily apply to schools and edtech providers. Most schools in the United States, including in California, are not organized for profit and instead are either nonprofit entities or subdivisions of the state or local government. Those schools, consequently, fall outside the CCPA's definition of "business," which requires an entity to be organized for profit.[35] Most edtech vendors, however, are for-profit entities.[36] Nonetheless, like the GDPR, the CCPA distinguishes between a "business" "on the behalf of which [personal] information is collected" and its agent, a "service provider" that "processes information on behalf of a business." Because edtech vendors collect and process personal information on behalf of schools, the applicability of the CCPA to edtech vendors depends on its treatment of principals and agents in the data lifecycle. We examine that treatment next.

---

28 Cal. Civil Code § 1798.140(c). The CCPA's definition of "business" also includes three alternative thresholds: annual gross revenues worldwide in excess of $25 million, processing the data of 50,000 or more consumers, or deriving more than fifty percent of its annual revenue from selling consumers' personal information. Id. § 1798.140(c)(1)(A)-(C).

29 Cal. Civil Code § 1798.140(g).

30 Cal. Civ. Code § 1798.140(g) (citing Cal. Code Regs. tit. 18, §17014).

31 Jehl, *supra* note 24; GDPR rec. 14.

32 See, e.g., 34 CFR 99.3 (defining "personally identifiable information" in part as "information that, alone or in combination, is linked or linkable to a specific student"); 45 CFR § 160.103 (defining "individually identifiable health information" in part as information for "which there is a reasonable basis to believe the information can be used to identify the individual); Erika McCallister et al., Nat'l Ins. of Stds. & Tech., Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) at 2-1 (2010), available at https://csrc.nist.gov/publications/detail/sp/800-122/final (defining PII as "any information that can be used to distinguish or trace an individual's identity . . . [or] any other information that is linked or linkable to an individual.").

33 Jacob Rubinstein, *A Close-Up on Deidentified Data Under CCPA*, IAPP (Aug. 27, 2019), https://iapp.org/news/a/a-close-up-on-de-identified-data-under-the-ccpa.

34 Cal. Civil Code § 1798.140(o)(1)(J) (citing 20 U.S.C. § 1232g; 34 C.F.R. Part 99).

35 However, schools receiving funding from the U.S. Department of Education, usually public schools, are subject to the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and myriad state student privacy laws, see *State Student Privacy Laws*, Student Privacy Compass, https://studentprivacycompass.org/state-laws/ (last visited Dec. 16, 2020).

36 See *List of EdTech Companies*, Crunchbase, https://www.crunchbase.com/hub/edtech-companies (last visited Nov. 20, 2020); Tony Wan, *Dozens of Venture-Backed Startups Among Edtech Recipients of PPP Loans*, Ed Surge (July 24, 2020), https://www.edsurge.com/news/2020-07-14-dozens-of-venture-backed-startups-among-edtech-recipients-of-ppp-loans.

IV. THE TRICKY SUBJECT OF PROCESSORS AND SERVICE PROVIDERS

A. Data Controllers and Data Processors under the GDPR

The GDPR and the CCPA both envision a two-tiered distinction between principals and agents in the data lifecycle. The GDPR categorizes principals and agents in the data lifecycle as "controllers" and "processors," respectively. A controller "determines the purposes and means of processing of personal data," while the processor "processes personal data on behalf of the controller."[37] Unlike under the CCPA, the GDPR's distinctions do not incorporate entities' for-profit status. A processor must be governed by a contract between the controller and the processor or by another legally binding act.[38] That contract must limit the "subject-matter and duration," "nature and purpose, "and categories of personal data and data subjects" of the processing.[39] The processor may "process[] the personal data only on documented instructions for the controller."[40]

Consequently, regardless of their for-profit status, schools and edtech vendors may qualify as controllers and processors, respectively. The relationship between a school and an edtech vendor may be described as one of principal and agent: the school provides student information to the vendor to provide the service such as online course materials or videoconferencing, and the vendor collects information on behalf of the school such as students' assignment submissions.[41] In that relationship, the school will define both the purposes and means of the processing; consequently, the school likely constitutes a controller and the edtech vendor a processor.

Edtech vendors, however, often collect and retain information for their own purposes and not on behalf of a school. For example, Summit Learning's privacy policy allows it to collect "de-identified" data, with all identifying data removed, for any purpose and to retain it indefinitely.[42] Similarly, Google's G-Suite for Education permits schools to allow students to use Google services beyond its core educational services; data collected from students using those "Additional Products" may be used for a variety of non-educational purposes such as customizing or developing new products.[43]

That collection may render an edtech vendor a "controller" under the GDPR. The European Data Protection Board ("EDPB") has suggested a processor acting "on behalf of" a controller "means that the processor may not carry out processing for its own purpose(s)."[44] The GDPR recognizes that processors might also collect or use data for their own purposes and provides, "[I]f a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing."[45] In such cases, the edtech vendor may qualify both as a processor and a controller, depending on if the data is processed on behalf of the school or for its own purposes.[46]

The GDPR also recognizes that two data controllers may qualify as "joint controllers." Edtech vendors and their school partners, however, may not qualify as a "joint controllers," due to divergent purposes and means of processing personal data. Under the GDPR, a "joint controller" is when "two or more controllers jointly determine the purposes and means of processing."[47] Joint controllers must provide a "transparent"

37 GDPR art. 4(6), (7).

38 GDPR art. 28(3).

39 *Id.*

40 *Id.* art. 28(3)(a).

41 Privacy Technical Assistance Center, U.S. Dep't Ed., Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices at 2 (Feb. 2014), available at https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-requirements-and-best.

42 *Data Privacy Addendum* § 4.5, Summit Learning, https://www.summitlearning.org/privacy-center/data-privacy-addendum (last visited Dec. 1, 2020).

43 *G Suite for Education Privacy Notice*, Google, https://workspace.google.com/intl/en/terms/education_privacy.html (last visited Nov. 23, 2020).

44 European Data Protection Board, Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR ¶ 79 (Sept. 2, 2020), *available at* https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en [hereinafter Guidelines 07/2020].

45 See GDPR art. 28(10).

46 *Data Processing Amendment to Google Workspace and/or Complementary Product Agreement (Version 2.3)* ¶ 5.3, Google, https://workspace.google.com/terms/dpa_terms.html (last visited Nov. 23, 2020) ("[T]his Data Processing Amendment does not apply to the processing of personal data in connection with the provision of any Additional Products.").

47 GDRP art. 26(1).

determination of responsibilities to comply with the GDPR, including in providing notice to data subjects.[48] The EDPB envisions that jointly determined purposes will either entail "the same, or common, purposes" or purposes that are "closely linked and complementary."[49] Similarly, jointly determined means requires each entity to "have exerted influence over the means of the processing," such as by agreeing to use a means of processing provided by one of the parties.[50]

An edtech vendor's use of student data for its own purposes is unlikely to meet those requirements, as the school and the vendor do not jointly determine either the purposes or the means of the processing. Instead, the schools merely utilize the data collected and forwarded by the vendor. The EDPB has suggested that merely "send[ing] personal data" is not sufficient to establish joint controllers.[51] For example, the EDPB describes an arrangement in which a "travel agency sends personal data of its customers to the airline and a chain of hotels, with a view to making reservations for a travel package"; each entity "processes the data for carrying out their own activities and using their own means."[52] Because there is no joint determination of means, the travel agency, airline, and hotel chain are likely not joint controllers. The same is likely true of an edtech vendor to the extent it uses student data for its own purposes and through its own means.

B. Service Providers under the CCPA

Although it makes a similar distinction between principals and agents, the CCPA's regime of "businesses" and "service providers" differs from the GDPR because it depends on an entity's for-profit status. As described above, a business under the CCPA is, among other requirements, a "legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information or on the behalf of which that information is collected."[53] Because most schools are not operated for profit, they do not fall within the scope of the CCPA.[54]

Edtech vendors, however, present a more complicated picture for two reasons. First, many edtech vendors would qualify as a business under the CCPA. As described above, many edtech vendors are for-profit entities and collect personal information. The collection is often for the vendor's own purposes, including research and the development of new products — non-educational uses that would likely be for the vendor's benefit rather than "on behalf of" its school partners. Similarly, a "business" under the CCPA must have annual gross revenues exceeding $25 million,[55] which the California Attorney General has clarified is worldwide revenue.[56] Many edtech vendors, especially the largest, clear that threshold.[57]

Second, that conclusion is complicated by the fact that edtech vendors are also working as agents on behalf of schools, which are not businesses. Like the GDPR, the CCPA recognizes a two-tier system of compliance for principals and agents. Whereas businesses are the primary focus of the CCPA, a "service provider" is a legal entity that "is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information."[58]

48 *Id.*

49 Guidelines 07/2020 ¶¶ 57-58.

50 *Id.* ¶¶ 62-63.

51 *Id.* ¶ 66.

52 *Id.*

53 Cal. Civil Code § 1798.140(c)(1).

54 Center for Analysis of Postsecondary Education and Employment, *Trends in Enrollment*, Columbia University (Feb. 2018), https://capseecenter.org/research/by-the-numbers/for-profit-college-infographic/.

55 Cal. Civil Code § 1798.140(c)(1)(A). Alternatively, a business that "annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers" or derives "50 percent or more of its annual revenues from selling consumers' personal information" will qualify as a "business." *Id.* § 1798.140(c)(1)(B)-(C).

56 Office of the Attorney General, Summary and Response to Comments Submitted During 45-Day Period, resp. 5 (June 1, 2020) [hereinafter 45-Day Response], available at https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf.

57 Tony Wan, *Earnings Roundup: How Public Edtech Companies Fared Following the Outbreak*, EdSurge (May 12, 2020), https://www.edsurge.com/news/2020-05-12-earnings-roundup-how-public-edtech-companies-fared-following-the-outbreak.

58 Cal. Civil Code § 1798.140(v) (emphasis added).

A business may disclose personal information to a service provider only pursuant to a written contract that, among other things, prohibits the service provider "from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified."[59]

Under those provisions, a service provider must process information "on behalf of a business." Thus, many edtech vendors would not qualify as "service providers" because the schools on whose behalf they process personal information do not qualify as businesses.

That conclusion, however, is altered by regulations recently promulgated by the California Attorney General, which alter the scope of a "service provider." Three of those regulatory provisions are relevant here.

First, the regulations provide that a business processing personal information on behalf of a nonprofit or public entity shall still be deemed a service provider. The regulations state, "A business that provides services to a person or organization that is not a business, and that would otherwise meet the requirements and obligations of a 'service provider' under the CCPA and these regulations, shall be deemed a service provider."[60] The Attorney General explained that this provision was necessary to avoid businesses providing services to nonprofits and public entities from being bound by the obligations the CCPA places on "businesses."[61] The Attorney General explained:

> For example, a public school district may use a service provider to secure student information, including each student's grades and disciplinary record. Without this regulation, service providers used by public and nonprofit entities may be required to disclose or delete records in response to consumer requests because they may constitute businesses that maintain consumers' personal information. Service providers for public and nonprofit entities could also be asked to disclose personal information maintained by a government agency, despite the fact that such files may be expressly exempt from disclosure under the Public Records Act.

Notably, this explanation assumes that entities that meet the CCPA's definitions of both "service provider" and "business" are only obligated to meet the obligations imposed on service providers, an assumption that is not expressly stated in the CCPA itself.[62] Thus, an edtech vendor providing services to a school may still qualify as a service provider and is likely not bound by the obligations imposed on businesses — at least to the extent the vendor is providing services to a school.

Second, the regulations clarify that an entity that collects data from or about consumers at the direction and on behalf of a business may still qualify as a "service provider."[63] The CCPA required entities to have personal information "disclose[d]" to them by a business to qualify as a service provider.[64] The Attorney General determined the statutory language was "incomplete" and added this regulatory provision to ensure that entities that collect information "as directed by or on behalf of a business" may still qualify as service providers, even if information is not disclosed to them by their business partners.[65]

The third regulatory provision clarifies "how entities that are both a service provider and a business are to handle consumer requests and other obligations under the CCPA."[66] The provision states, "A service provider that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider."[67] Thus, an edtech vendor that collects or processes information for its own purposes will be deemed a business under the CCPA for that collection or processing, subject to the

---

59 *Id.*

60 Cal. Code Regs. tit. 11, § 999.314(a).

61 Office of the Attorney General, Final Statement of Reasons at 30 (June 1, 2020) [hereinafter Final Statement of Reasons], *available at* https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf.

62 See 45-Day Response, resp. 555; Office of the Attorney General, Initial Statement of Reasons at 23 (Oct. 11, 2019) [hereinafter Initial Statement of Reasons], https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.

63 Cal. Code Regs. tit. 11, § 999.314(b).

64 Cal. Civil Code § 1798.140(v).

65 Initial Statement of Reasons at 21.

66 *Id.* at 23.

67 Cal. Code Regs. tit. 11, § 999.314(f).

corresponding obligations. The implication from this provision is that an entity is not bound by the CCPA's business provisions[68] with respect to the processing it provides as a service provider.

The sum result of these regulatory provisions is that for-profit edtech vendors may still qualify as service providers even if they (1) are processing personal information on behalf of not-for-profit entities, (2) are collecting information from or about consumers, so long as they do so on behalf of and at the direction of a business, and (3) otherwise qualify as a business under the CCPA, but any information processed outside the scope of their functions as a service provider is subject to the CCPA's business obligations.

V. IMPLICATION FOR DATA RIGHTS

Ultimately, the geographic scope, substantive applicability, and principal-agent distinction determine who is responsible for ensuring that individuals can exercise their data rights. Both the GDPR and the CCPA provide persons with rights to data deletion, disclosure of collection and sharing practices, opt-out or objection to certain data uses, and nondiscrimination for exercising their rights. Both also require businesses or controllers to obtain affirmative consent regarding certain processing of personal information from children younger than 16.[69] The GDPR carries additional rights to data minimization, rectification, portability, and disclosure of automated decision making.

Under both laws, the principal in the data lifecycle — the "controller" under the GDPR and the "business" under the CCPA — carry the primary responsibility for exercising those rights. Both laws require the controller or business to notify data subjects and consumers of their statutory rights and to facilitate requests for data access, deletion, opt-out or objection, and correction, among others.

In contrast, the responsibilities of processors and service providers are more limited and more contractual in nature. The GDPR requires that processors "be governed by a contract . . . that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller."[70] With respect to data subjects' data rights, however, a processor must merely "assist[] the controller . . . for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights."[71] The CCPA regulations specifically permit service providers to decline to honor requests made by consumers or to direct the consumers to the corresponding business.[72] Like the GDPR, the CCPA requires the service provider to operate under a written contract that "prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract."[73]

Thus, under either law, an edtech vendor must be cognizant of when it is processing data as a "business" under the CCPA or as "controller" under the GDPR; in those cases, it must provide consumers with the required notices and respond to requests by consumers to exercise their data rights. As a "service provider" or "processor," the vendor does not necessarily have those responsibilities, but must still operate within the contractual requirements imposed by the laws.

VI. CONCLUSION

Technology and data have played an increasing role in education, a trend that has been amplified by the pandemic and remote learning. Although the GDPR and CCPA may seem uniquely suited to the privacy concerns posed by edtech, their application depends on a number of factors, and edtech vendors should be aware of the laws' geographic reach, substantive scope, and distinctions between principals and agents in the data lifecycle.

68 Cal. Civil Code § 1798.100-.135.

69 Cal. Civil Code § 1798.120(c) (affirmative consent to opt-in to the sale of PI); GDPR art. 8(1) (parental consent must be provided for any processing for children under 16).

70 GDPR art. 28(3).

71 GDPR art. 28(3)(e).

72 Cal. Code Regs. tit. 11, § 999.314(e).

73 Cal. Civil Code § 1798.140.

CPI COMPETITION POLICY INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.